PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04M

A2

(11) International Publication Number: WO 91/01067

(43) International Publication Date: 24 January 1991 (24.01.91)

(21) International Application Number: PCT/US90/03290

(22) International Filing Date: 14 June 1990 (14.06.90)

(30) Priority data:
378,721 12 July 1989 (12.07.89) US

(71) Applicant: MOTOROLA, INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: FLANDERS, Mary, Beth ; 202 Hillcrest, Wood Dale, IL 60191 (US). PUHL, Larry, C. ; 6 Plum Court, Sleepy Hollow, IL 60067 (US).

(74) Agents: PARMELEE, Steven, G. et al.; Motorola, Inc., Intellectual Property Department, 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

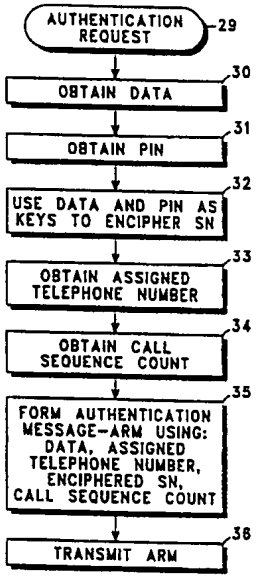
(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent)*, DK (European patent), ES (European patent), FR (European patent), GB (European patent), IT (European patent), JP, KR, LU (European patent), NL (European patent), SE (European patent).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD FOR AUTHENTICATION AND PROTECTION OF SUBSCRIBERS IN TELECOMMUNICATION SYSTEMS

(57) Abstract

Radio frequency based cellular telecommunication systems often require a subscriber to maintain a proprietary identifier or serial number which is transmitted to a fixed network communication unit to verify the authenticity of the subscriber. Unauthorized detection of these proprietary ID's is substantially decreased by this invention. This invention describes an enciphering method and call sequencing method, which when combined, provides substantial protection for the subscriber against unauthorized detection of their proprietary identifiers.



* See back of page

DESIGNATIONS OF "DE"

Until further notice, any designation of "DE" in any international application whose international filing date is prior to October 3, 1990, shall have effect in the territory of the Federal Republic of Germany with the exception of the territory of the former German Democratic Republic.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MC	Monaco
AU	Australia	FI	Finland	MG	Madagascar
BB	Barbados	FR	France	ML	Mali
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Fasso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GR	Greece	NL	Netherlands
BJ	Benin	HU	Hungary	NO	Norway
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	SD	Sudan
CF	Central African Republic	KP	Democratic People's Republic of Korea	SE	Sweden
CG	Congo			SN	Senegal
CH	Switzerland	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
DE	Germany, Federal Republic of	LK	Sri Lanka	TG	Togo
DK	Denmark	LU	Luxembourg	US	United States of America

METHOD FOR AUTHENTICATION AND PROTECTION OF SUBSCRIBERS IN TELECOMMUNICATION SYSTEMS.

TECHNICAL FIELD

This invention relates generally to communication systems and more particularly to radio frequency (RF) cellular telecommunication systems.

BACKGROUND OF THE INVENTION

Cellular radio telephone systems typically include subscriber units (such as mobile or portable units) which communicate with a fixed network communication unit via RF transmissions. A typical fixed communication network includes at least a base station and a switching center. One responsibility of the fixed network communication unit is to grant use of the communication system to the subscriber unit after the requesting subscriber unit meets the authentication requirements of the system. In a typical cellular telephone communication system, each subscriber unit is assigned a telephone number (mobile identification number) (MIN) and an identification number (or serial number) (SN) which uniquely identifies the subscriber to any fixed network communication unit. Each subscriber unit has a unique identification number that distinguishes it from other subscriber units. The fixed network communication unit has access to these identification numbers through a database. Often these numbers are used by the fixed network communication units to bill subscribers for the time the subscriber uses the system. When the subscriber calls another unit, he enters the phone number he wishes to call. The dialed phone number becomes the data to be sent to

the fixed network communication unit. Data may also include other information regarding a third communication unit such as a unit's location.

Detection of a legitimate subscriber's identification number may be accomplished by RF eavesdropping or by purposeful or inadvertent divulgence of the MIN/SN combination by the radio telephone installer. Once the subscriber's telephone number and identification number is known (stolen), a thief may reprogram another subscriber unit with the stolen identification number causing two or more subscriber units to have the same MIN/SN combination. Cellular radio telephone systems have authentication procedures to deny access to subscribers not having legitimate identification numbers, but do not have the capability to detect multiple users or effectively neutralize the effect of an installer leaking subscriber identification numbers. Therefore, the legitimate user is billed for both the thief's use and his own use.

Several authentication techniques are known. EIA-553 section 2.3 specifies that each subscriber shall have a MIN and a factory set SN. The telephone number which the subscriber is attempting to contact is the data that is transmitted by the subscriber to the fixed network communication unit. Authentication is granted by this system if the MIN and corresponding SN are found in the fixed network communication unit database. Unfortunately, EIA-553 does not require the encipherment of the MIN or SN before transmission to the fixed network communication unit thereby permitting direct RF detection of any MIN or SN. In addition, this technique fails to provide protection against a thief that acquires a MIN/SN from an installer.

Another authentication technique is described in European cellular communication system recommendations generated by the Groupe Special Mobile (GSM); see sections:

02.09, 02.17, 03.20, and 12.03. This method additionally requires the subscriber to openly transmit a temporary mobile subscriber ID (TMSI) to the fixed network communication unit; the fixed network communication unit generates and sends a random number (RAND) to the subscriber. The enciphering technique requires the subscriber unit to autonomously retrieve at least three enciphering elements from its memory: a predetermined ciphering key, an SN (individual subscriber authentication key) and a MIN (international mobile subscriber identification number - IMSI). The subscriber then enciphers its SN and MIN using the cipher to construct the RAND into a signed response (SRES). The subscriber unit transmits this signed response back to the fixed network communication unit where the fixed network communication unit checks the SN, MIN, and ciphering key against its database using the subscriber's temporary ID (TMSI).

The fixed network communication unit generates its response to the same random number using the information retrieved from the database and compares the subscriber signed response to the fixed network communication unit generated response. If the responses are substantially equivalent, authentication is confirmed. The dialed telephone number is only allowed to be transmitted after authentication is granted. This system affords some protection against a thief that acquires the MIN/SN from an installer by enciphering the SN and reassigning a temporary TMSI each time the subscriber enters a different cell area.

Although one technique enciphers the subscriber's serial number before transmission, neither system detects multiple users. Detection of thieves once they acquire access is important to maintaining a secure system. Moreover, the random number transmission (required for encipherment) necessitates additional communication between the subscriber unit and the fixed network communication unit each time a call

is made which increases the probability of transmission error and adds a transmission step to the fixed network communication unit's authentication protocol routine. In addition, authentication must be verified before the system will allow data to be accepted. Therefore data must be sent after the steps of the authentication procedure are complete.

There exists a need for a substantially enhanced authentication technique for a cellular telecommunication system that detects fraudulent users and efficiently protects identification numbers from unauthorized detection. The authentication method should restrict an illegitimate user's capacity to utilize the system in the case where access is inadvertently granted. Further, an adequate level of security resulting from encipherment should not require additional transmission processes or inject higher error levels during the authentication process.

BRIEF SUMMARY OF THE INVENTION

These needs and others are substantially met through provision of the method for authentication and protection of subscribers in telecommunication systems disclosed below. This method describes an authentication technique for use between a first communication unit, such as a subscriber unit, and a second communication unit, such as a fixed network communication unit, wherein the first communication unit modifies an ID, known to both the first communication unit and the second communication unit (such as a serial number), using data as one enciphering key and a second ID (such as a Personal Identification Number - PIN) as the other enciphering key. An historic non-arbitrary value of predetermined communication events, such as a count of the number of telephone calls made

by a subscriber, is maintained in both the first and second communication units. This value (count) is historic because it represents past telephone calls attributed to a communication unit, and it is non-arbitrary because this history of transactions (i.e., number of calls made) serves to identify an out-of-sync communication unit.

The first communication unit transmits (via RF signals) the modified ID and count to a second communication unit. The second communication unit compares the count maintained by the first communication unit to the count maintained by the second unit. A count discrepancy indicates a different number of calls on one unit indicating a multiple user whose count is out of sequence. The second communication unit performs the same enciphering method on the known serial number using the data received and a known second ID. The second communication unit compares the received modified serial number and the serial number generated by the fixed network communication unit to determine if the serial number is valid. The invention is designed to substantially decrease unauthorized use of a first ID of a communication unit. The authentication method does not require the second ID to ever be transmitted by RF.

This invention provides a means for detecting multiple subscribers using the same serial numbers and telephone numbers. Moreover, if a multiple user copies the information transmitted and uses the same information to access the system, the multiple user will be limited to only calling the telephone number that is in the authentication message; not a telephone number of his own choice. This authentication invention also reduces authentication errors by making more efficient use of the data transmitted and a second ID, by using them as a part of the cipher; the enciphering means does not require an additional RAND stream to be sent by a fixed network communication unit to be used as the common

enciphering base and thereby eliminates this additional transmission and therefore decreases the probability of errors.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a typical subscriber communication unit and fixed network communication unit.
FIG. 2 is a flow chart of the identification enciphering method used by a subscriber communication unit.
FIG. 3 is a flow chart of the authentication method used by a fixed network communication unit in accordance with the invention.

BEST MODE OF OPERATION

FIG. 1 generally depicts a subscriber communication unit (10) such as a subscriber telephone and a fixed network communication unit (20) such as a cellular telephone basesite and switching center. The subscriber communication unit (10) is comprised of a microprocessing stage (12), a non-volatile memory unit (11), a radio frequency (RF) stage (13), all as well understood in the art. Additional elements include a data input stage (14) such as a key entry pad on a telephone (to enter a telephone number - data), a subscriber call sequence counter (15), and an output from an enciphering stage referred to as the enciphered serial number (16).

Within the non-volatile memory unit (11) resides the serial number (18) (for the subscriber unit), the PIN (19), and the subscriber telephone number (17) (which can have, for example, characteristics of a Mobile Identification Number (MIN)). The PIN is a second ID known only to the subscriber unit and the fixed network unit. For example, it should not be available to an installer of the subscriber unit, it should only be available to a legitimate user of a subscriber unit and a

fixed network communication unit database. The subscriber need only enter the PIN one time to activate it. The PIN may be changed by the subscriber, but the change must also be made known to the fixed network unit. These identifiers need not necessarily be numbers but may correspond to any attribute capable of being identified by the fixed network communications unit. An alternative embodiment, for example, in a cellular system, may include a stored look up table containing multiple sets of serial numbers, PIN's, and telephone numbers with each set of identifiers corresponding to a specific cellular area or fixed network communication unit.

The fixed network communication unit (20) includes a switching center which is comprised of a microprocessing stage (22), a database (23), and a link to a basesite radio frequency stage (21), all as well understood in the art. Additional elements include a fixed network unit call sequence counter (24) and an enciphered serial number generated by the fixed network unit (25).

The database includes information regarding the subscriber unit's: serial number (28), PIN (27), and subscriber telephone number (26); the information includes a stored copy of the serial number (28), PIN (27), and the subscriber telephone number (26). The serial number (18), PIN (19), and telephone number (17) of the subscriber communication unit (10) correspond to the serial number (28), PIN (27), and telephone number (26) as stored in the fixed network communication unit (20). Communication between the subscriber communication unit (10) and the fixed network communication unit (20) is accomplished via RF transmissions between the two units in accordance with well understood cellular system techniques.

When authentication is required of the subscriber communication unit (10), the subscriber unit enciphers its

serial number (18) and increments its call sequence counter (15). FIG. 2 depicts the method used by a subscriber communication unit to encipher its serial number before transmission to a fixed network communication unit during an authentication request (29). This method requires use of two enciphering keys. The subscriber unit obtains the called telephone number (data) (30) and obtains PIN (31) from memory and uses at least parts of these two components as the enciphering keys to encipher its serial number (32). If PIN and the called telephone number are comprised of bits, the parts of these keys to be used are the contents of the bits and the bit length of each key. For example, an enciphered serial number may have a different bit length than the unenciphered serial number, or unmodified first ID, depending on the contents of the PIN or the data. Varying the enciphered SN bit length may also be a function of another event known to both the subscriber and fixed network unit such as the time of day.

The algorithm to integrate the two enciphering keys may be varied to accommodate various levels of security depending upon the requirement of the system. The subscriber identification enciphering method does not require authentication to be confirmed by the fixed network communication unit before data is transmitted. Combining PIN with data adds the ability of the system to encipher a serial number into a complex code to an extent sufficient to substantially eliminate unauthorized detection by RF eavesdropping and unauthorized divulgence by installers.

The modified serial number (enciphered SN) becomes a component of the Authentication Request Message (ARM) (35) that is transmitted via RF (36) to the fixed network communication unit. Once encipherment is complete, the assigned telephone number is obtained (33) from memory. This number is not enciphered as part of the authentication procedure. This identifier is a component of the ARM (35) that

informs the fixed network unit that the authentication request is coming from a valid subscriber unit.

The call sequence count is then obtained (34) and also used in the ARM (35). The call sequence count is updated (incremented or decremented) each time a predetermined event occurs such as when the authentication procedure is initiated or a call is completed. The count may be maintained by the subscriber and fixed network unit using a rollover type counter such as a ring counter. This count is used by the fixed network communication unit as a means to count the number of calls made by each subscriber. Because a record of the number of calls made by each subscriber is maintained by both the subscriber unit and the fixed network communication unit, another subscriber trying to use the same serial number will be detected because it will not have made the exact same number of calls as the legitimate subscriber. The call sequence count information is communicated to the fixed network unit as one component of the Authentication Request Message. The ARM can be communicated in any acceptable format or in any number of stages. Components of a typical ARM (35) include data, the enciphered serial number, the call sequence count, and the assigned telephone number. An alternative embodiment would include modifying the call sequence count using the same enciphering method that is used to modify the SN. This would further enhance the protection because the count is also disguised using the PIN and data; each subscriber would generate a different value for the same count (number of calls made).

A fixed network communication unit receives a transmitted ARM and uses this information to determine whether authentication should be granted to the subscriber unit. FIG. 3 depicts the authentication method performed by a fixed network unit. The ARM is received (37) by the fixed network unit by means of the base RF unit (21). The fixed

network unit has access to assigned telephone number's, serial number's and PIN's of valid subscriber units through its database. The fixed network unit determines if the assigned telephone number received in the ARM is valid (39) by obtaining from the fixed network unit database the same assigned telephone number (38). A comparison is made between the received telephone number from the subscriber unit and the valid number found in the database (39). If the assigned telephone number is not recognized by the fixed network unit, authentication is denied (or some other action taken) (40).

If the assigned telephone number is determined to be valid (it is found in the database), the fixed network unit then retrieves from the database the serial number and PIN corresponding to that particular assigned telephone number. The fixed network unit then, uses the PIN from the database and the data received in the ARM as enciphering keys as elements of its enciphering method (44), which is the same method used in the subscriber unit, and generates its own enciphered serial number. The fixed network unit compares this enciphered serial number to the serial number enciphered by the subscriber unit(46). If they are not substantially the same, then the system denies access or takes some other predetermined course of action (47). If they are within the acceptable tolerance, the received call sequence count is obtained (48) and compared (50) to the call count maintained by the fixed network communication unit (49). If the counts are substantially equal, authentication may be confirmed (52) which is the first predetermined course of action. At this point, the subscriber may be allowed to communicate with the third communication unit associated with the dialed number. This third unit may more generally be termed a requested communication resource. If the count is not within the acceptable tolerance, authentication may be denied or the

authorities may be notified that a multiple user is attempting to access the system (51).

The fixed network unit call counter maintains the number of times authentication is granted to a subscriber. Each subscriber has its own call counter. Having a continuous call counting scheme between a subscriber and a fixed network communication unit prevents another subscriber from using some other subscriber's identification number because the thief would not have made the identical number of calls that the legitimate subscriber made. This discrepancy is flagged by the fixed network unit when it compares the two counts.

Protection against illegitimate users is further enhanced by the encipherment method's use of the enciphered dialed telephone number and the PIN (which is not transmitted). Without an illegitimate user knowing a subscriber's PIN and the exact algorithm that enciphers the serial number, a thief is limited to merely copying the authentication message of a subscriber and repeating this message. Each time a subscriber dials a different telephone number, a different authentication request message is generated because each subscriber has a different PIN; each subscriber generates a different authentication request message for the same telephone number.

Although a thief may detect the call sequence count (because it is not enciphered in the ARM) and update it, a correct count would only allow the thief to gain authentication for the enciphered dialed telephone number he intercepted. Therefore the illegitimate user can only communicate to the subscriber whose enciphered telephone number matches that copied from the ARM.

An alternative embodiment comprising the call sequence count may allow each subscriber to maintain more than one call counter where a separate call counter is required for each fixed network communication unit. This embodiment would

find use in a cellular communication system which allowed a subscriber to use multiple fixed network communication units. Another alternative embodiment to the flow in FIG. 3 may require the step of comparing the call sequence counts (50) to occur before the step involving the comparison of enciphered serial numbers (46).

CLAIMS

What we claim is:

1. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:

A) providing the first communication unit with at least one ID and data, having post authentication utility, to be transmitted;

B) providing the second communication unit with information regarding the ID;

C) in the first communication unit, modifying the ID at least in part as a function of at least part of the data, having post authentication utility, to be transmitted to provide a modified ID;

D) transmitting, from the first communication unit to the second communication unit, at least the modified ID and at least part of the data, having post authentication utility, to be transmitted.

2. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:

A) providing the first communication unit with at least a first and second ID and data, having post authentication utility, to be transmitted;

B) providing the second communication unit with information regarding the first and second ID;

C) in the first communication unit, modifying the first ID as a function of at least part of the data, having post authentication utility, to be transmitted and the second ID to provide a modified first ID;

D) transmitting, from the first communication unit to the second communication unit, at least the modified first ID and at least part of the data, having post authentication utility, to be transmitted.

3. The method of claim 2 wherein the second ID is not transmitted in the transmitting step.

4. The method of claim 1 or 2 wherein the data, having post authentication utility, to be transmitted includes at least identifying information regarding a third communication unit.

5. The method of claim 4 wherein the identifying information includes a telephone number.

6. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:

A) maintaining an historic non-arbitrary value in both the first and second communication units, of predetermined communication events as between the first and second communication units;

B) transmitting, at least from time to time, from the first communication unit to the second communication unit, count information as maintained by the first communication unit;

C) receiving, at the second communication unit, the historic non-arbitrary value information;

D) comparing, at the second communication unit, the historic non-arbitrary value information as received from the first communication unit with count information as maintained by the second communication unit;

E) when the historic non-arbitrary value information as received from the first communication unit is substantially the same as the historic non-arbitrary value information as maintained by the second communication unit, taking a first predetermined course of action;

F) when the historic non-arbitrary value information as received from the first communication unit is substantially different from the historic non-arbitrary value information as maintained by the second communication unit, taking a second predetermined course of action.

7. The method of claim 6 wherein the first predetermined course of action includes providing the first communication unit with a requested communication resource.

8. The method of claim 6 wherein the historic non-arbitrary value may be a count.

9. The method of claim 6 wherein the predetermined communication events are comprised of the telephone calls attributed to the first communication unit.

10. The method of claim 6 wherein the historic non-arbitrary value is maintained by a ring counter.

11. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:

A) providing the first communication unit with at least one ID, data, having post authentication utility, and an historic non-arbitrary value to be transmitted;

B) providing the second communication unit with information regarding the ID;

C) in the first communication unit, modifying the ID and the historic non-arbitrary value at least in part as a function of at least part of the data, having post authentication utility, to be transmitted to provide a modified ID and a modified historic non-arbitrary value;

D) transmitting, from the first communication unit to the second communication unit, at least the modified ID, the modified historic non-arbitrary value, and at least part of the data, having post authentication utility, to be transmitted.

12. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:

A) providing the first communication unit with at least a first, a second ID, an historic non-arbitrary value, and data, having post authentication utility, to be transmitted;

B) providing the second communication unit with information regarding the first and second ID;

C) in the first communication unit, modifying the first ID and the historic non-arbitrary value as a function of at least part of the data, having post authentication utility, to be transmitted and the second ID to provide a modified first ID and a modified historic non-arbitrary value;

D) transmitting, from the first communication unit to the second communication unit, at least the modified first ID, the modified historic non-arbitrary value, and at least part of the data, having post authentication utility, to be transmitted.

13. A method for facilitating communications between a first communication unit and a second communication unit, comprising the steps of:

A) providing the first communication unit with at least a first and second ID;

B) providing the second communication unit with information regarding the first and second ID;

C) in the first communication unit, modifying the first ID as a function of an event, known to both the first communication unit and the second communication unit, resulting in a modified first ID with at least a modified attribute of the unmodified first ID;

D) transmitting, from the first communication unit to the second communication unit, at least the modified first ID;

E) receiving, at the second communication unit, at least the modified first ID;

F) in the second communication unit, modifying the first ID as a function of an event, known to both the first communication unit and the second communication unit, resulting in a modified first ID with at least a modified attribute of an unmodified first ID;

G) comparing, at the second communication unit, the modified first ID as received from the first communication unit with the modified first ID generated by the second communication unit;

H) when then modified first ID as received from the first communication unit is substantially the same as the modified first ID as generated by the second communication unit, taking a first predetermined course of action;

I) when the modified first ID as received from the first communication unit is substantially different from the modified first ID as generated by the second communication unit, taking a second predetermined course of action.

14. The method of Claim 13 wherein the modified attribute of the first ID is comprised of a modified bit length of the unmodified first ID.

15. The method of Claim 13 wherein the event known is data, having post authentication utility, communicated.

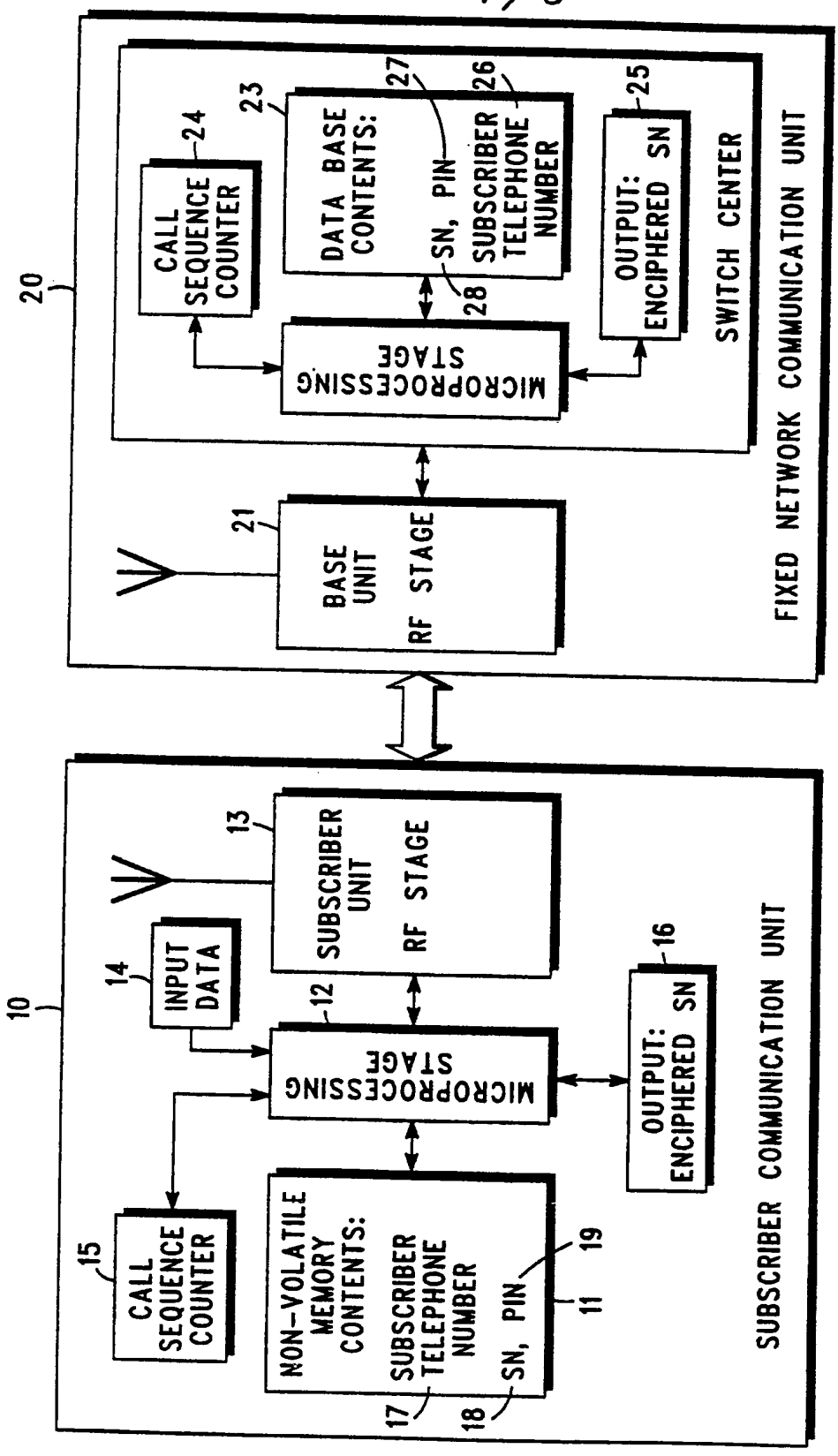

FIXED NETWORK COMMUNICATION UNIT
SWITCH CENTER
20
CALL SEQUENCE COUNTER
24
DATA BASE CONTENTS:
23
SN, PIN
27
SUBSCRIBER TELEPHONE NUMBER
26
OUTPUT: ENCIPHERED SN
25
28
MICROPROCESSING STAGE
BASE UNIT RF STAGE
21
SUBSCRIBER COMMUNICATION UNIT
10
SUBSCRIBER UNIT RF STAGE
13
INPUT DATA
14
12
MICROPROCESSING STAGE
OUTPUT: ENCIPHERED SN
16
CALL SEQUENCE COUNTER
15
NON-VOLATILE MEMORY CONTENTS:
SUBSCRIBER TELEPHONE NUMBER
17
SN, PIN
18
19
11

FIG. 1

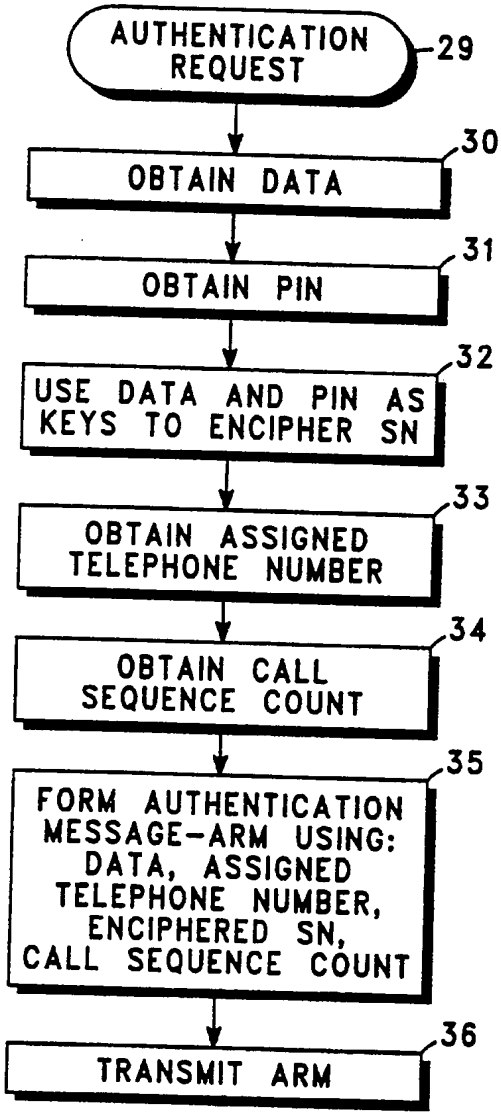

AUTHENTICATION REQUEST
29
OBTAIN DATA
30
OBTAIN PIN
31
USE DATA AND PIN AS KEYS TO ENCIPHER SN
32
OBTAIN ASSIGNED TELEPHONE NUMBER
33
OBTAIN CALL SEQUENCE COUNT
34
FORM AUTHENTICATION MESSAGE-ARM USING: DATA, ASSIGNED TELEPHONE NUMBER, ENCIPHERED SN, CALL SEQUENCE COUNT
35
TRANSMIT ARM
36

FIG. 2

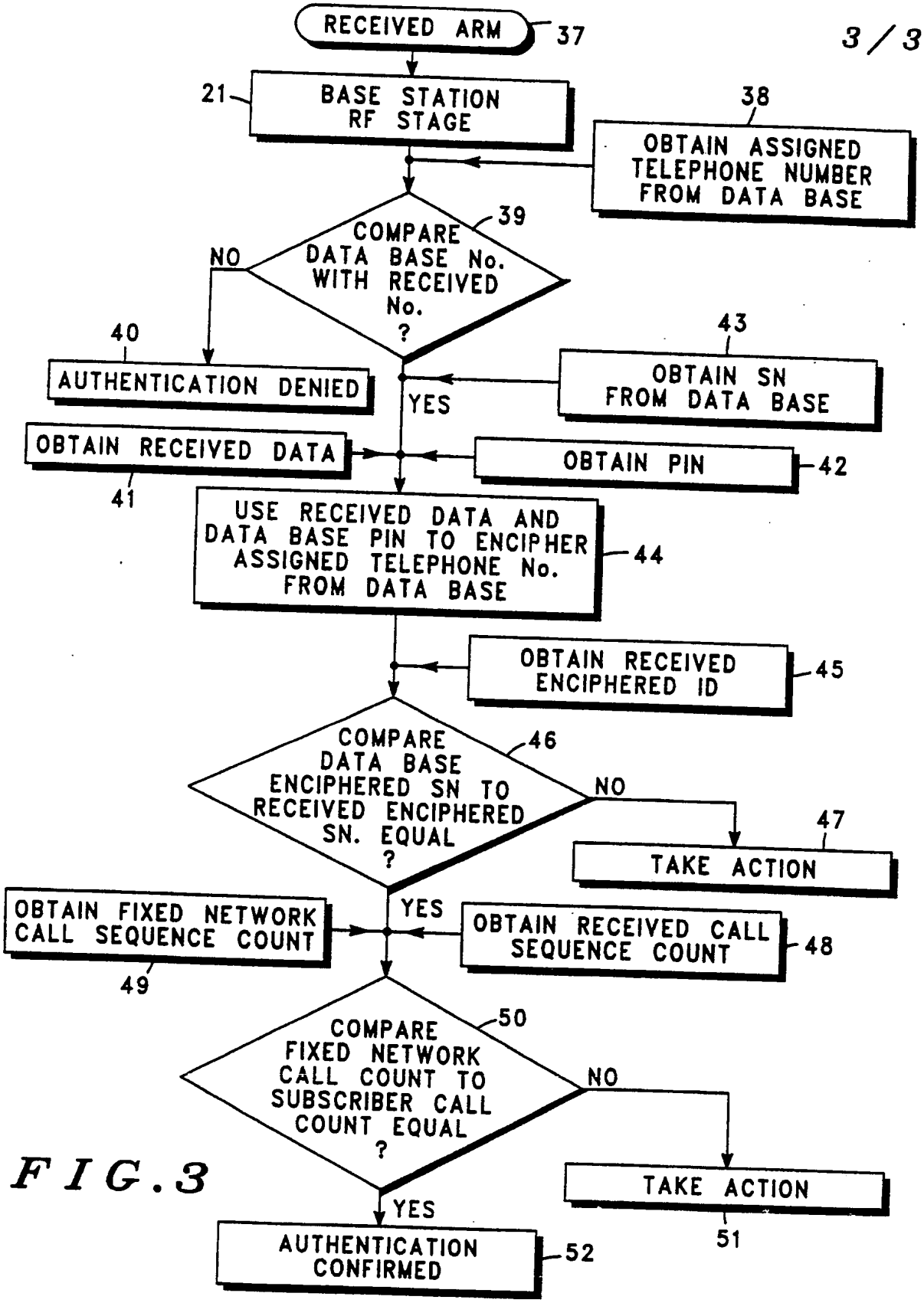

RECEIVED ARM
37
21
BASE STATION RF STAGE
38
OBTAIN ASSIGNED TELEPHONE NUMBER FROM DATA BASE
39
COMPARE DATA BASE No. WITH RECEIVED No. ?
NO
40
AUTHENTICATION DENIED
YES
43
OBTAIN SN FROM DATA BASE
OBTAIN RECEIVED DATA
41
OBTAIN PIN
42
USE RECEIVED DATA AND DATA BASE PIN TO ENCIPHER ASSIGNED TELEPHONE No. FROM DATA BASE
44
OBTAIN RECEIVED ENCIPHERED ID
45
COMPARE DATA BASE ENCIPHERED SN TO RECEIVED ENCIPHERED SN. EQUAL ?
46
NO
47
TAKE ACTION
YES
OBTAIN FIXED NETWORK CALL SEQUENCE COUNT
49
OBTAIN RECEIVED CALL SEQUENCE COUNT
48
COMPARE FIXED NETWORK CALL COUNT TO SUBSCRIBER CALL COUNT EQUAL ?
50
NO
TAKE ACTION
51
YES
AUTHENTICATION CONFIRMED
52

FIG. 3